DEVELOPMENT FIELD

Security of Broadband Access Network

Wang Deqiang
(Network Division of ZTE Corporation, Shanghai 201203, China)

Abstract:
Due to the rapid development of broadband access technologies, the broadband access networks have wider and wider application. However, with the development, the security issue became a public concern. Under the environment of access network, customers, access equipment and networks all face various threats, especially those from the user side. Such technologies and solutions as port positioning, fraud prevention on Medium Access Control (MAC) addresses and monitoring of illegal services might be the solution to the security problem existing in the current networks.

In the late ten years, the broadband access network is getting popular all over the world. Increasing number of people and entertainments access the Internet through broadband. The users are no longer satisfied by the high performance of access. They are having higher requirements on service quality. In company with the Quality of Service (QoS), one of the most important is security.

1 Security Issues of Access Network

In time, the technology of broadband access network significantly matured, which makes possible the Internet access for increasing number of users. Meanwhile, the increase of users intensifies the possibility of attack on network, especially after large-scale deployment of Ethernet and IP technology. The share-oriented Ethernet has its advantages as well as obvious shortages. There are numerous hack tools, which could be used to threaten the network, for example, snoop the network, steal the service, launch the Deny Of Service (DOS) attack[1], break down the network, and more. Originally, IP network was not designed for the public, therefore, no security problems were considered. Most of the services are completed by intelligent terminals, which were out of the control of carriers. The carrier's responsibility is limited for transporting data packets from one device to another. Monitoring the services is not easy, which created ideal environment for hackers.

In order to provide an access network of telecommunication carrier level, the equipment vendors and carriers should focus their attentions on how to provide secure access services[2–3]. To date, there are several access technologies, including Digital Subscriber Line (DSL), Hybrid Fiber Coaxial (HFC), Passive Optical Network (PON) and WiMax (Worldwide Interoperability for Microwave Access). They share similar architecture as shown in Figure 1.

The architecture of broadband access networks consists of the following components:

(1) Customer Premises Network

The customer premises network is a kind of Local Area Network (LAN) which uses Customer Premises Equipment (CPE) as the core. This network belongs to the users. The DSL is the most popular access approach currently.

(2) Access Node

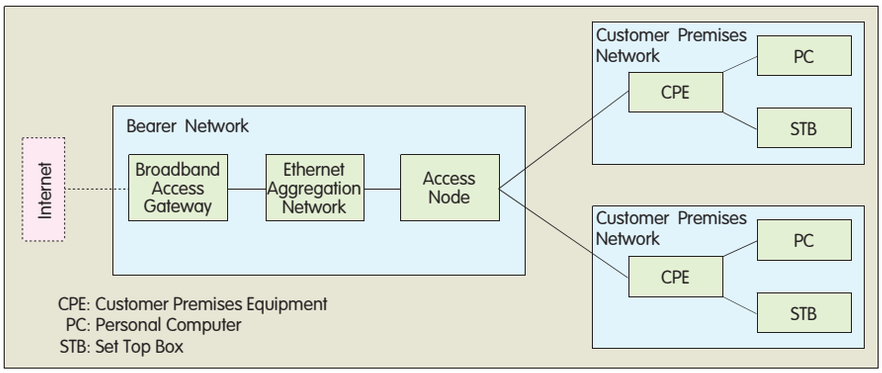
The Access Node (AN) terminates the loops or wireless channels and aggregates the user data. The main purpose of the AN is to accept users with more possible variant access approaches. As the boundary of carriers' network, the AN is the closest equipment to users. It is the first gate the user data gets through first. Therefore, the AN plays an important role in solving network security problems.

(3) Ethernet Aggregate Network

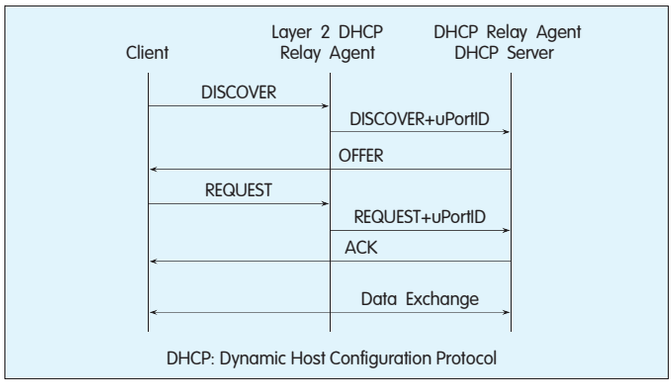
The Ethernet network has its advantage of low cost and high performance. Numerous carriers have chosen it to deploy. Moreover, the Ethernet aggregate network aggregates and switches the user data.

(4) Broadband Network Gateway

The Broadband Network Gateway (BNG) could have many



▲ Figure 1. Architecture of broadband access network.



▲ Figure 2. Process of DHCP Option82.

functions: physical encapsulation termination, user authentication, user terminal auto-configuration, and QoS guarantee. The BNG could be one device, or be several devices. It works as a remote broadband access server, a Dynamic Host Configuration Protocol (DHCP) server (or a DHCP relay) and router.

The AN, the Ethernet aggregate network and the BNG belong to carriers, which means they could be trusted by carriers. As the customer premises networks belong to the users, the carriers can not trust them. Normally, network attacks come from malign users or programs in trustless network.

In summary, the following security problems exist in the access network.

- Access of illegal users.
- Illegal packets and malign packets.
- MAC/IP spoofing.
- Illegal services, such as illegal VoIP and illegal access in secret.

The mentioned problems will be discussed in the following with corresponding solutions.

2 Access of Illegal Users

The illegal user access decreases the carriers' income greatly. Without identifying and authenticating the users, illegal access could be seen everywhere.

The user identification and authentication turns out to be a mature technology. Radius over Point-to-Point Protocol over Ethernet (PPPoE), DHCP+Web and 802.1x protocol are commonly deployed. Presently, the identification of loop line is the concern. Under retail environment, every user has a corresponding logic port in access node. For wired network, it is the hardware port, while for wireless network the soft port. If only user name is to be identified, it is possible for the user to share its user name and password with unauthorized users, which is unacceptable to the carriers.

In Point-to-Point Protocol over Asynchronous Transfer Mode (PPPoA) access environment, every user has its unique Virtual Channel (VC), which is terminated at the Broadband Remote Access Server (BRAS). Therefore, the user's logical port information could be found directly on BRAS.

Currently, the PPPoE and IP over Asynchronous Transfer Mode (IPoA) are the main access approaches. The user loops and the VCs are terminated at ANs. Sometimes, there is even no VC. The BRAS can not get the logical user port information directly. Therefore, an efficency mechanism should be adopted to send the user' logical port information to BRAS. Presently, several user port identification solutions have been provided.

(1) Protocol DHCP Option82

The Protocol DHCP Option82 is described in RFC 3046, which is fully based on RFC 2131 (DHCP). The DHCP Option82 extends the protocol process. At the access node, the DHCP protocol packets will be captured according to DHCP Option82. In direction of upstream, user port information must be inserted into DHCP protocol packets as Option82. In direction of downstream, user port information in DHCP protocol packets may be omitted optionally. Figure 2 demonstrates the process of DHCP Option82.

(2) Protocol PPPoE+

The Protocol PPPoE+, also known as the PPPoE intermediate agent, extends the packets of PPPoE protocol. As DHCP Option82, in direction of upstream, PPPoE+ captures PPPoE packets and inserts user port information. Figure 3 demonstrates the process of PPPoE+.

(3) Protocol VBAS

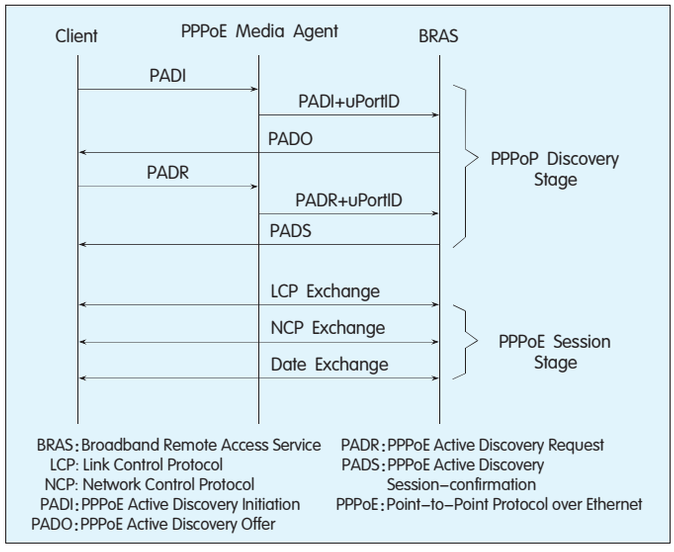
Dissimilarly to PPPoE+, the Virtual Broadband Access Server (VBAS) changes the steps of PPPoE process. It adds two steps between BRAS and AN in order to insert user port information. Figure 4 demonstrates the process of VBAS.

(4) VLAN Stacking

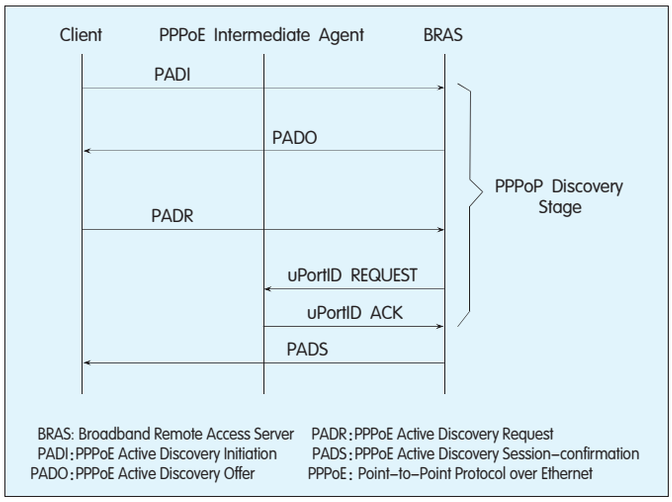
Compared with conventional Virtual Local Area Network (VLAN) technologies, the VLAN Stacking uses double VLAN tag. The outer tag plays the same role with conventional VLAN while the inner tag carries the user port information.

(5) Virtual MAC

The source MAC address in every packet will be translated based on predefined rules according to Virtual Media Access Control (VMAC). The translated MAC is unique and contains port information. In this way, when BRAS processes PPPoE packets, it can get port information directly from the source MAC address.



▲ Figure 3. Process of PPPoE+.



▲ Figure 4. Process of VBAS.

Table 1 makes a contrast among the mentioned solutions.

3 Illegal and Overload Packets

As the customer premises networks are out of control, malign users or programs could send illegal protocol packets upstream, which decrease the performance of upper network equipment. In worse situation, it could disorder the equipment or shut it down. Besides, if malign users or programs send lots of protocols or broadcast packets, regardless of whether they are legal or not, it could consume significant precious equipment resources.

In direction of downstream, although the network devices are trusted, it can not be guaranteed the equipment will work correctly.

Illegal packet includes:

(1) Packets with illegal source MAC address. The source MAC address can not be broadcast or multicast address, or some predefined MAC addresses conserved for specific purpose.

(2) Illegal protocol packets. Practically, in direction of upstream, it's impossible for Internet Group Management Protocol (IGMP) to receive QUERY packets. In direction of downstream, the IGMP can not receive REPORT, LEAVE or JOIN packets. For DHCP there is no OFFER or ACK packets in direction of upstream and no DISCOVER or REQUEST packets in direction of downstream. As for PPPoE, it could not receive PADO or PADS packets in direction of upstream, PADI or PADR in direction of downstream. All these packets should be filtered.

(3) Jumbo packets, mini packets or packets with error checksum. Normally, packets with length less than 64 bytes or more than 1 518 bytes should be filtered. In specific situation, jumbo packets are acceptable.

The filters are used to filter illegal packets. The theory of filter is very simple. It predefines the pattern of illegal packets. When packet comes, the filter uses the pattern to match the packet. If it matches, the packet is filtered, otherwise it passes. Presently, most of the switch chips have the capability of pattern defining and packet matching function.

Overload packets have the following types:

- Overload protocol packets.
- Overload broadcast packets.
- Overload multicast packets.
- Overload packets with different source MAC addresses.

The first three types are supposed to consume equipment resources greatly; the fourth type will possess the limited MAC address table resource.

Filtering the first three types has the following steps:

(1) Predefine the pattern of packets that are supposed to be filtered and the maximum speed of packets flow.

(2) When a packet comes, find its corresponding pattern, and compute the speed of the pattern.

(3) If the speed is larger than the predefined speed, drop the packet.

The technology of processing overload protocol, broadcast and unicast packets is called packet refrain.

It is comparatively simple to solve the problem of overload source MAC address. Maximum number of MAC address could be configured at every port. In this way, every packet with new MAC address will be dropped after maximum numbers of MAC addresses have been learned.

Every component in the network should filter overload and illegal packets, especially for the ANs because of their location.

4 MAC/IP Address Spoofing

The MAC/IP address spoofing threatens the safety of network severely.

The MAC/IP address spoofing comes when switch receives packets with identical MAC address from different port. When this happens, the host has to be relocated. In a malign way, some users will be kicked out.

Two types of MAC spoofing could be categorized: the user side MAC address spoofing and the network service server side MAC address spoofing. The service server includes BRAS, DHCP server/relay, default gateway, and more.

In LAN, the MAC address of Ethernet could be scanned by any user/program. If packets with identical MAC address get into different ports, this will confuse the MAC learning and cause some users be denied by the network.

▼ Table 1. Contrast among port location solutions

Solution	DHCP Option82/PPPoE+	VBAS	VLAN Stacking	VMAC
Strengths	DHCP/PPPoE is extended without extra exchange steps of original protocols.	Extensibility can be used to control QoS and user bandwidth.	No protocol exchange and no interference on higher protocols.	No protocol exchange steps, with a higher security.
Weaknesses	DHCP protocol packets need real time analysis. There is no standard port information formats.	It has a complicated configuration as one DSLAM and one VLAN, supporting PPPoE only.	It's required to support layer 2 VLAN with many requirements on equipment.	MAC-related protocols are required to be considered.

DHCP: Dynamic Host Configuration Protocol
PPPoE: Point-to-Point Protocol over Ethernet
VBAS: Virtual Broadband Access Server
VLAN: Virtual Local Area Network
VMAC: Virtual Media Access Control

In order to enhance security, in access network, user port isolation is required at the AN. User port isolation means user ports in the same VLAN can not exchange information, but they can exchange information with uplink port. Presently, the technology of Private Virtual Local Area Network (PVLAN) is used for this purpose.

Not all switch chips support PVLAN. Even when PVLAN is supported, the problem of MAC duplicate will still happen if MAC address configuration is set incorrectly. User's MAC address could be got in some way, such as brute-force attack. In a word, PVLAN can not solve the problem of MAC address spoofing.

The following ways can be used to solve the problem:

(1) VMAC

At AN, in direction of upstream, every combination <physical port, MAC> is assigned a unique virtual MAC address. The virtual MAC address can be trusted because it's created by the AN. In addition, the MAC address duplicate is guaranteed not to exist. In direction of downstream, according to the translating table, the VMAC address can be converted back to the original MAC address. The VMAC can not only be used to solve MAC address spoofing, but also can be used to identify user. However, the VMAC will interfere with some protocols related with MAC.

(2) MAC Address Bonding

It binds the MAC address to user port statically. Packets with different MAC address from the bound address will be dropped. Although this way is very simple, its usability is bad. Customer premises network has variant MAC addresses. This method is difficult to manage.

(3) Packet Switch Based on PPPoE Session Aware

In PPPoE access environment, every user has a unique PPPoE session identification. A table <PPPoE session id, port> can be used at AN. The packets are aggregated upstream. In direction of downstream, the packets are switched according to this table. In this way, it is no necessary to use MAC address table. Therefore, there will be no MAC duplication problem.

(4) Packet Switch Based on IP Aware.

In IP over Ethernet (IPoE) access environment, at AN, a table <IP address, port> can be used. Every user has a unique IP address and will be no IP duplication problem. In direction of downstream, packets can be switched according to the table. Similarly to packet switch based on PPPoE session aware, no MAC address learning is needed.

The mentioned third and fourth methods have requirements on upstream VLAN. If every AN has a unique upstream VLAN, there is no problem. However, if several ANs share a same upstream VLAN, upstream aggregative switch connected to these access nodes has to switch packets in the same way. The use of PPPoE session and IP address is a different way from traditional switch to switch packets. For a normal switch chip, it's hard to fully support PPPoE session or IP aware packet switch.

Service server's MAC address spoofing can lead to migration of service server's MAC address and most of users connected to the equipment will be rejected. The following methods can be used to solve this problem:

(1) VMAC

As described, the VMAC can be used to solve MAC address spoofing in all access environments.

(2) Service Server's MAC Address Static Configuration

Manually configure the service server's MAC address into the static MAC address list of the AN switch. In this way, it is impossible to migrate the MAC address learning at AN. This method is very simple, but its extensibility and flexibility are quite bad.

(3) Service Server's MAC Address Auto Configuration

This method was provided by the author. The basic theory is that let the AN work as PPPoE client or DHCP client, which sends PPPoE or DHCP requests regularly. In this way, access node can get BRAS's MAC address or DHCP server/relay's MAC address dynamically. It has obvious advantages. It uses the present protocols without manual configuration. It won't modify any protocol packets and claim extra requirements from other protocols.

IP address spoofing happens in IPoE access environment to steal other users' services. Or some users use IP addresses not assigned by the DHCP server/relay. This is an obstacle for the carrier to manage the whole network. One way to solve this problem is implementing "DHCP IP source guard" at AN. This guard monitors DHCP protocol packets between DHCP client and server. It guarantees that before a user gets configuration, all other packets from/to the user will be dropped. Once getting DHCP ACK, it binds the assigned IP address and the user's MAC address to the user port. And then, the coming packets from/to the user port will be checked with the bound <IP address, MAC address>. When the lease of DHCP expires, cancel the bond, and stop transporting all packets except for DHCP from/to this user port.

5 Illegal Service

After years of access network construction, for the carriers, the broadband is not the main problem any more. Presently, there are two important concerns. One is how to provide more services and changing the profit approaches based only on access and broadband. The other is how to control the illegal services.

The illegal services are defined by carriers. If a service is not provided by carriers, and it is in interference with the services provided by carriers, it is considered an illegal service.

The main illegal services include:

(1) P2P downloads. The P2P download consumes lots of broadband. It makes network too busy to be accessed by legal users.

(2) VoIP. The VoIP has diverted a lot of users from Public Switched Telephone Network (PSTN). This could dampen the income of carrier greatly.

(3) Illegal broadband share. User applied the broadband access in the name of family user originally. But after that, it is used by entertainment or network bar, or shared among several families. This also decreases the income of the carriers.

Dissimilarly to the other security problems described previously, illegal services have complicated features. It is difficult to filter the illegal packets just based on simple match. In order to check whether a flow is illegal or not, it is necessary to

analyze the data flow deeply based on predefined feature information database. It is impossible to decide an illegal packet only based on the packet information. The decision is based on the data flow. Therefore, the equipment has to be able to memorize the information of the data flow.

It is common to use Network Address Translator (NAT) at modem in order to share broadband among several families and/or entertainment. In this way, to the carrier, it seems just one user is connected to the access node. Solving this problem it is required to collect and analyze all trails. That is, to analyze connecting numbers of Transmission Control Protocol (TCP), communication throughout, source TCP port range. Moreover, to analyze some specific personal information carried in MSN or Windows update packets, operating system version and IE version in upstream packets. Usually, it is necessary to combine all these collected information to make a final decision. This can reduce the possibility of incorrect decision.

It is difficult to find out illegal VoIP because so many VoIP softwares exist. Different software has different features. In order to get through firewall or NAT, some VoIP softwares use special port to launch VoIP service in private channel. All User Datagram Protocol (UDP)/TCP packets have to be monitored. It is necessary to use the features in the process of VoIP registering, connecting and accessing.

The features of P2P data flow are easy to be defined because the number of P2P software is comparatively small.

Practically, illegal service checking could be implemented at all layers of the network. The lower the layer is, the easier to get higher performance. However, it has to suffer from the higher cost and more difficulty of management.

Illegal service detection has a trend of intelligence. It rewards greatly because it can create a high added value. As access network is used increasingly, illegal service detection will be commonly deployed. It represents an important research direction.

6 Conclusions

As for commercial applications in access network, security problems are unavoidable and changeable. Not only the carries pay much attention to security problems, but the telecommunication equipment vendors also think much of them. As a top three access network vendor in the world, ZTE provides a full solution to solve the discussed security problems.

References

[1] PIKE J. Cisco **网络安全**[M]. **北京**: **清华大学出版社**, 2004.
[2] **鲍淑娣**, **沈连丰**. **宽带无线接入带来的机遇与挑战**[J]. **中兴通讯技术**,2004,10(3): 36–39.
[3] **周武**旸, **毛雪鸿**. **固定宽带无线接入技术的发展**[J]. **中兴通讯技术**, 2004,10(3): 1–4.

Manuscript received: 2006–04–18

Biography

Wang Deqiang graduated from Nanjing University with his Doctor's degree. He is a system engineer at the Third System Department of Network Division of ZTE. He is engaged into R&D of network products. He has published ten technical papers, and applied five invention patents.

Roundup

Vodafone Signs Handset Procurement Agreement with China's ZTE

Vodafone Group and ZTE Corporation announced a handset procurement agreement which will see the Chinese company produce a range of Vodafone–only branded, ultra–low cost handsets for sale across Vodafone's Markets.

The handsets will only carry the Vodafone name, adding to the range of devices which Vodafone offers branded in this way for the consumer market, and marks the continuation of Vodafone's Original Design Manufacturers' strategy, which is intended to bring to market high–quality and low–cost devices under the Vodafone name.

Vodafone anticipates offering the first Vodafone–branded, ZTE–manufactured handset, a 2G ultra–low cost device, created particularly for sale in Emerging Markets, in the second quarter of 2007.

Jens Schulte–Bockum, Vodafone's Global Director of Terminals said: "Vodafone's Original Design Manufacturer strategy is intended to use Vodafone's size and purchasing power to engage with the best white label handset makers and then use the power of the Vodafone brand to bring their products to market. We are pleased that we have signed this agreement with ZTE which will build on their experience in emerging markets to create for us an ultra–low cost handset as the first of a range of products we seek to develop with them."

He Shiyou, senior vice president of ZTE added: "This agreement with one of the world's largest mobile operators is a breakthrough for us and highlights ZTE's ability to develop handsets according to European Operators' requirements and standards. Vodafone's requirements include world class design and quality standards combined with competitive cost structures. The signing of this agreement has demonstrated ZTE's capability and commitment to fulfill these requirements and deliver volumes meeting the needs of a world class operator." (ZTE)